9/290363

0758348 BW0017

IMPROVENET: A Match Made On The Internet : Improvenet.com Helps Contractors Build Their Businesses

October 15, 1997

Byline: Business Editors
Dateline: PALO ALTO, Calif.
Time: 04:55 PT
Word Count: 682

FEATURE...

PALO ALTO, Calif.--(BUSINESS WIRE FEATURES)--Oct. 15, 1997--Pennsylvania contractor Phil Coggeshall knows that in the building and home remodeling business, it really is a jungle out there. Hard-working, reliable contractors often fight a stereotype created by their con-artist counterparts. That's why he believes it's crucial to separate the good guys from the bad!

"We're seeing a lot more garbage and crime in the industry these days. Slick scammers are setting up companies that take advantage of people," Coggeshall says. "It's important that homeowners have a sense of security. They need to be able to protect themselves financially."

Coggeshall has now armed himself with what he believes is the most valuable marketing tool around: Improvenet (http://www.improvenet.com), a new, free Internet-based service that helps match homeowners to qualified contractors who stand apart from the rest.

For a fraction of what it costs to advertise in the yellow pages or newspaper, ImproveNet offers pre-screened, licensed contractors the chance to thoroughly describe their expertise, elaborate on their credentials, list references and display photos of their work 24 hours a day, 7 days a week!

"I've been in the business for fifteen years as a member of the Pennsylvania Builders Association, the local affiliate for the National Home Builders Association. At first, I was a little apprehensive about doing business over the Internet," Coggeshall says. "Referrals and handshakes have always been the name of the game, but the Internet is a great resource to help attract customers. You're appealing to upscale homeowners who need real help and are willing to pay for quality work. You're attracting people who can appreciate what you have to offer."

"For appropriately qualified contractors, ImproveNet can serve as the sales and marketing arm of their small business," says Kelly Conway, vice president of sales at ImproveNet. "ImproveNet is attracting significant and lucrative jobs every day from homeowners who need a contractor immediately. Since ImproveNet provides a detailed description of the project, tradespeople can effectively pre-screen the calls they wish to pursue and only target those jobs they are most interested in bidding and working on."

William Cline, a contractor from Ben Lomand, California, agrees. Cline, a twenty-year veteran in the business, has already secured three jobs through ImproveNet. He's very pleased with the screening process that weeds out unsavory contractors and wish-washy consumers as well. "ImproveNet makes life easier for the contractor and the homeowner," Cline says. "While working on a job I was referred to through ImproveNet, the homeowner told me someone from the company was periodically checking in to make sure everything was running smoothly. I found that to be very impressive. I knew ImproveNet thoroughly checked out my references; what I didn't know was that they would follow through with my client to make sure my work was up to par. I think that's great."

>

Cline also likes the fact that the homeowners are pre-qualified, too. 'I waste a lot of time and money running out to do estimates on a 'remodeling project' that turns out to be a dishwasher installation," Cline says. "With ImproveNet, the homeowner has thought about the project, given a thorough description of his needs and is serious about the work. That's the way it should be!"

And ImproveNet is not just about jobs. It's about savings. "ImproveNet delivers value-added programs to its network of pre-screened and pre-qualified contractors," says Conway. "These include discounts on critical components of any contractor's business like cellular phones, paging services and insurance."

For Phil Coggeshall, ImproveNet is opening up new windows of opportunity. The benefits reach far beyond fear of this new, evolving technology. "I think every contractor should have a computer and incorporate their business strategies with the Internet. ImproveNet is the future. It's exciting, it's great!"

It's great news for good guys like Coggeshall and Cline. Bad news for the bad guys.

CONTACT: Pacifico
Christine Pullara or Marilyn Nix
408/293-8600
cpullara@pacifico.com
mnix@pacifico.com
or
ImproveNet
Bob Citelli
(415/650) 322-1197
rjc@improvenet.com

KEYWORD: CALIFORNIA

INDUSTRY KEYWORD: BUILDING/CONSTRUCTION

0901904 BW0014

IMPROVENET 2: ImproveNet Launches ContractorWatch: **A Free, Nationwide Contractor Quality Tracking Network For Homeowners**

September 02, 1998

Byline: Business Editors
Dateline: SAN FRANCISCO
Time: 03:02 PT
Word Count: 614

SAN FRANCISCO--(BUSINESS WIRE)--Sept. 2, 1998--The overwhelming majority of professionals in the home improvement industry are skilled, hard working and honest.

But a relatively small number have given the $180 billion industry a bad reputation with homeowners. A new, free Internet-based service called ContractorWatch(tm) has been launched to help homeowners avoid getting stuck with a poor quality or unscrupulous contractor. ContractorWatch is the first national, contractor-tracking network of its kind.

ContractorWatch is sponsored by ImproveNet (www.ImproveNet.com), America's leading independent service matching homeowners with reliable contractors, architects and lenders. ContractorWatch is accessed through a link on ImproveNet's site.

A Local and National "Contractor-Scape"

For the first time, homeowners have a local and national view of the quality of nearly any contractor in the country that has three or more years experience. ContractorWatch will use ImproveNet's database of over 650,000 professionals. A homeowner visiting ImproveNet's website (www.ImproveNet.com) can simply enter his or her zip code to display: 1) The total number of contractors, designers and architects in that region 2) The total number of professionals screened "good." 3) The total number of professionals screened "bad."

If homeowners have already selected a contractor and want to obtain current credit and legal history, not available on any other site, a fee of $29 is charged for a faxed report.

Remodelers, who are just starting a project and are in need of a quality contractor in their area, can quickly complete a free, project request form and receive data on up to four contractors who have met ImproveNet's rigorous screening criteria. ImproveNet's criteria include a professional's credit and legal history, current contractor license, insurance and references. Since individual contractors must be alerted to a specific bid opportunity and allowed to respond to ImproveNet, a homeowner can expect the contractor names and contact information in about 12-36 hours.

ContractorWatch Scam Alert

Another part of the free ContractorWatch service focuses on home improvement-type frauds dealing with lending and refinancing, inspection, roofing, painting, siding, driveways, and general remodeling. Each major scam and its M.O. (modus operandi) is explained in detail, updated when variations are uncovered. Homeowners can view national scams or see the latest frauds on a state-by-state basis.

They can also report home improvement fraud in their own areas through ImproveNet's ScamSighting(tm) Report. A simple online form is used to capture scam information that is compiled and summarized on the ContractorWatch portion of the company's website.

In addition to individual homeowners providing scam information, ImproveNet is in weekly contact with state attorneys general offices and local police departments throughout the United States. This information allows ImproveNet to continuously monitor scams.

About ImproveNet

ImproveNet Inc. (www.ImproveNet.com) is the Internet's leading

independent service helping homeowners find reliable contractors, architects and lenders. ImproveNet's database contains information on more than 650,000 contractors, architects and designers nationally. The company matches homeowners with remodeling and design experts in their local area who have passed a rigorous proprietary screening test. The key criteria evaluated by ImproveNet's proprietary screening system are credit history, legal judgements, license status (if required by local or state laws) and insurance. ImproveNet's web site also features a visual gallery of design ideas created by leading architects and designers as well as practical advice from home improvement experts.

For more information, contact Chris Kane, ImproveNet (www.improvenet.com), 1286 Oddstad Drive, Redwood City, CA., 94063, 650/261-0661 ext.217, cmkane@improvenet.com, Bob Morse or John Starkweather, MorseMcFadden Communications, 425/889-0528, bobm@morsepr.com and johns@morsepr.com.

CONTACT: ImproveNet
Chris Kane, 650/261-0661 x217
cmkane@improvenet.com
or
MorseMcFadden Communications
Bob Morse or John Starkweather
425/889-0528
bobm@morsepr.com
johns@morsepr.com

KEYWORD: CALIFORNIA

INDUSTRY KEYWORD: COMED COMPUTERS/ELECTRONICS REAL ESTATE INTERACTIVE/MULTIMEDIA/INTERNET

Today's News On The Net - Business Wire's full file on the Internet with Hyperlinks to your home page.
URL: http://www.businesswire.com

0781673 BW0287

IMPROVENET: ImproveNet.com Now Matches Homeowners to Pre-screened Architects and Designers; America's Home Improvement Network Answers Consumer Demand for More Help With Home Remodeling

December 04, 1997

Byline: Business & Home/Garden Editors and Real Estate/Computer Writers
Dateline: PALO ALTO, Calif.
Time: 15:07 PT
Word Count: 515

PALO ALTO, Calif.--(BUSINESS WIRE)--Dec. 4, 1997--ImproveNet, today announced the expansion of its free online matching service for homeowners to include a new database of over 7,000 architects and designers.

Professionals from across the country were selected for superior quality and reputation by experts and consumers. Improvenet (www.improvement.com) is the nation's largest online independent service bringing together homeowners, reliable contractors, lenders, and other home and garden professionals.

A recent survey conducted by San Francisco's Consumer Action shows remodeling disasters rank as one of the biggest complaints by consumers. ImproveNet's matching services hope to eliminate the problem by finding the best in the business for homeowner needs.

"Homeowners engaged in major home improvement projects should consult an experienced architect or professional designer because they are much more likely to get the results they desire" said Bob Stevens, president of ImproveNet. "A large percentage (20%) of homeowners who come to us looking for a contractor have also expressed an interest in professional design assistance. An architect, kitchen and bath, or landscape, or designer, is a space and planning problem-solver who can help crystallize a homeowner's remodeling project in ways that may not occur to the homeowner or might be overlooked by the contractor."

ImproveNet's designers and architects come with the highest recommendations from colleagues and associates in the home and design remodeling community. Consumer referrals also play a major role in which professionals are recommended.

"A proven professional will have the respect of his peers and customers, and that's a key indicator that the person belongs in our proprietary database," adds Stevens. "Our automated systems contact local designers and architects and match them to appropriate jobs." A homeowner simply types in his home improvement need online; ImproveNet then emails out a list of three to six professionals in the area who are interested and available to work within the homeowner's time frame. Services are also available toll-free at 888-8IMPROV.

"By consulting with a respected designer or architect, not only is the job likely to proceed much more smoothly, but costly mistakes can easily be avoided that would otherwise lead to additional expense and distress for the parties involved," said Stevens.

ImproveNet has processed more than $100 million in construction projects referrals through its Web site at www.improvenet.com. Consumers using the service have saved between $10 million and $12 million on projects processed during the first three quarters of 1997.

About ImproveNet

ImproveNet is on the World Wide Web at http://www.improvenet.com, or can be reached at 888-8IMPROV. The colorful Web site, updated frequently, features free matching service for homeowners in need of reliable contractors, designers, architects, and financial lenders.

In addition, the site offers home and garden design ideas, planning tips, home product news and information, and advice from experts.

Note to Editors: For screenshots, user stories and other requests, contact Marilyn Nix, Pacifico 408/293-8600.

CONTACT: Pacifico
Marilyn Nix, 408/293-8600
mnix@pacifico.com
or
ImproveNet
Bob Citelli, 650/322-1197
rjc@improvenet.com

KEYWORD: CALIFORNIA

INDUSTRY KEYWORD: COMPUTERS/ELECTRONICS COMED INTERACTIVE/MULTIMEDIA/INTERNET REAL ESTATE PRODUCT

Today's News On The Net - Business Wire's full file on the Internet with Hyperlinks to your home page.
URL: http://www.businesswire.com

9/482840

EDNSept 26, 2002

Prying eyes: the greatest door lock in the world is ineffective if you leave the key under the mat. With cryptographic keys so strong, why break them when they're so much easier to steal? (Cover Story).

Author/s: Nicholas Cravotta

MOST PEOPLE WHO BUILD or use today's supposedly secure systems have fallen under the illusion that complex encryption algorithms are enough to protect data. As a consequence, they leave their data or keys protecting their data exposed for theft.

A key component of any secure system is the physical security of the electronics involved. Because logical attacks, such as breaking a cryptographic key, are infeasible, attacking a system physically becomes an appealing option. Once someone gains physical access to equipment, stealing sensitive information can be as simple as attaching a scope. Depending on the sensitivity of information your system will process, you might also consider some of the ways you can make your designs physically more resistant to such attacks.

SETTING YOUR BOUNDARIES

Perhaps the most important decision you can make is how you set your security boundary, which defines the parts of your system that are secure and the parts that are not. Access across the boundary between secure and nonsecure subsystems is limited and protected. For example, unencrypted cryptographic keys should never cross the security boundary; therefore, they can never be copied. Without a security boundary, an application might have access to keys, which means someone could instead choose to break the application to copy and misuse the keys.

If you too broadly define your security boundary-say you want to place an entire rack of boards behind the boundary--validating that you haven't unintentionally left "implementation holes" through which an attacker could compromise the system becomes a daunting task. You can also too narrowly define your security boundary. For

example, it does little good to protect just a chip if the data coming into the chip is exposed; nobody would bother to break the chip when he or she could just lift the information off of the interface to the chip. Thus, few security chips offer much physical security, and the security boundary is typically an entire board or module.

You also need to consider who might attack your device and why. Someone may just be having fun or making a statement about individual freedom. The attacker may care not about the information gained by possessing certain keys but about the ability to impersonate or spoof legitimate users of those keys. The attacker may even be a competitor who wants to copy your design (see sidebar "Protecting IP").

Your primary defense is to raise the cost of breaking the system to a value greater than the potential payoff. When breaching the security boundary is difficult, the attempt becomes less appealing. Another strategy is based on "outrunning the lion": When running away from a lion, you don't necessarily have to run faster than the lion; you just have to run faster than the guy next to you. Often, to avoid being a target, you need only to make your system less profitable to break than your competitor's.

Bear in mind that many layers of security boundaries exist. If the security boundary of the room housing the board is sufficient, you need not secure the board. The reality is, however, that human factors ten make otherwise-secure boundaries vulnerable (see sidebar "Human factors"). The best boundaries put people outside them (Figure 1a). Give a password to a person, and he or she will probably write it down somewhere in a nonsecure location, thus compromising the information that the password protects.
[FIGURE 1 OMITTED]

Interfaces across a security boundary are a favorite target for attack. Any device that you can upgrade, for example, stands the risk of being hijacked by an attacker's spoofed upgrade. Spoofed code could duplicate unencrypted traffic, such that every packet the board processes is also sent to the attacker. One method of protecting against such an attack is called red/black separation (Figure 1b). "Red" refers to plain data, and "black" refers to cipher data. Typically, red and black data travel over the same bus when the same processor handles both types of data, making it possible--through corrupt code, design error, or environmental stress--to send red data over a black port. Separating red and black processing into different subsystems reduces the chance of this kind of error's occurring. If you can't separate the subsystems, you may want to self-monitor your traffic to see whether you are occasionally sending red data to the wrong port.

Once you set your security boundary, you need to define how your system will react to breaches. The simplest strategy for a board is to make it tamper-resistant, by, for example, covering it with opaque

potting material so an attacker can see neither its contents nor their location (Figure 1c). A higher level of protection is to make your board "tamper-evident" (Figure 1d); in other words, design your board so that, when someone attacks it, he or she leaves evidence. Think of this evidence as a broken seal on a letter. However, such evidence may reveal only that someone made an attempt--not whether the attempt was successful. Tamper-evident defenses must be outside the security boundary; you don't want to have to compromise the boundary to see whether someone has compromised it. The evidence must also be irreversible and protected. In other words, the attacker should be unable to dispose of the evidence.

The next level of protection is to make your board "tamper-respondent" (Figure 1e). The board must be able to detect tampering and act independently, usually to destroy whatever sensitive material it contains before it can be compromised. Note you must also protect the tamper-respondent subsystem, which resides within the security boundary, from attack. The highest level of protection is robust tamper resistance against attacks such as extreme temperatures, drilling, X-rays, and chemicals. You usually achieve this protection using a tamper-respondent mesh (see sidebar "Tamper-respondent sensors").

Some types of protection may not apply to your needs. You can also overprotect a system by implementing protection at a cost that outweighs the value of the protected information. Creating a board with too much security also makes the board difficult to debug and manufacture. Be aware that attackers can use test points on a board, which are useful for quickly testing a board during manufacturing, to explore or even reprogram the board. Potting the points may temporarily hinder someone from using them for such purposes.

MADNESS TO THE METHOD

Once you define your security needs, you need to understand what it takes to achieve such a level of assurance. One of the best ways to find out is by studying the various methods and schemes that attackers may use to compromise your system (see sidebars "Chip-level defense: processors" "Chip-level defense: memory," "Board-level defense," and "Power attacks"). Some attacks require expertise or equipment. You may determine that the person attacking your system doesn't have these resources available, because anyone with that kind of equipment is seeking to attack a system that will yield significantly more value than yours does. In such cases, you may comfortably decide to leave your system vulnerable.

The FIPS (Federal Information Processing Standard) 140 standard defines various levels of defense that a system must deploy. Your customers may not require FIPS compliance from your product, although some may ask for it in ignorance, but reviewing the standard may still be worth your time. Unless you have experience

with attacks, you may be unable to properly evaluate how realistic a threat they are to you. For example, do you know whether it is difficult to mill off the top of an IC package and probe a diet Do you know how safe the proprietary secrets of your chip are from someone who wants to reverse-engineer them? And do you know how difficult and effective a liquid-nitrogen attack is? Have you ever even heard of one?

Attackers can quickly compromise some systems while a board is active. Others, such as those using X-ray machines, assume that an attacker has been able to later extract the board for evaluation at his or her lab of choice. Boards that respond when someone removes them without authorization increase the difficulty of a leisurely attack.

You sometimes know your attacker. In the set-top-box industry, for example, attackers are often subscribers! Thus, the secure box is in the attacker's lab of choice, and he or she can dissect it at leisure. Building a tamper-evident box is difficult, because you cannot see the physically altered box. You may be able to detect an abnormality when you communicate with the box, but the attacker is likely to anticipate and protect against that scenario. One argument says that a guy in his garage threatening to steal $40 in premium channels isn't a threat. He becomes a threat, however, when he posts information about how to do it on the Web: The visitor counter at one such Web site, www.pirateden.com, claims more than 11 million visitors since March 2001. Certainly, laws exist to protect equipment such as set-top boxes, but their effectiveness at preventing theft is unclear. You'd be better off making modifications to your equipment more difficult than the payoff warrants.

Various security standards are in place. NIST (National Institute of Standards and Technology) manages the North American standard for cryptographic modules, FIPS 140. Common Criteria is a worldwide standard. The CSE (Communications Security Establishment) manages the Canadian standard, and the CESG (Communications Electronics Security Group) manages the British standard.
NIST recently released Version 2 of the FIPS 140 standard, which will supersede the FIPS 140-1 standard by the end of this year. FIPS 140-2 focuses on clarifying ambiguities rather than changing methods. (See Reference 1 for the proceedings of a recent conference on differences, between 140-1 and 140-2.)Because the FIPS 140 specs contain little numerical information, they seem vague. Therefore, you must work out some of the details with a consultant or with the test house that will validate your design. Test houses must validate their test systems with NIST, so a high level of consistency should exist among them. In any case, the NIST document on derived test requirements is essential reading for all designers (Reference 2).

Don't expect to walk up to a test house and present a finished black

box for validation. The intimacy of the testing process depends on whether you need Level 1 (weak) or Level 4 (strong) validation. For example, a potential attacker of a Level 4 military board could have the financial backing of an entire nation. Additionally, an attacker could be a former employee who perhaps served as chief architect of the design he or she is attacking. For maximum security, you must assume that an attacker has access to all of a design's notes, tools, and documentation. If your device is truly secure, even an attacker with this information should fail. This concept is based on the theory that knowing the encryption algorithm shouldn't make it any easier to break keys or, to paraphrase Kerchkhoff's Principle, the security of a cryptosystem must not depend on a secret.

Thus, for the highest level of security, you must expose your entire design and design process--from philosophy, through hardware schematics, to fully documented code listings--to the test house. Obviously, this process will involve secrecy and nondisclosure agreements. If you are uncomfortable with such dealings, then don't consider a high level of FIPS validation.

The test house will require you to provide a policy statement defining how you operate the device, the environment in which it exists, its functions, the security boundary, and so on. In the early design stages, the test house should suggest design methodologies that will later speed the approval process, and it points out potential implementation holes. Once you prototype devices, the test house will want to destroy a few. If a device fails any of the test-house trials, you have to modify the device and prove to the test house that you've corrected the problem.

Some companies employ consultants before approaching a test house. One reason for doing so is to have another set of critical eyes searching for implementation holes. A second reason is that doing so makes it more difficult for you to pay off the test house to let an implementation hole slip through testing--a reassurance that might be important to your final customer.

Note that software plays a large role in FIPS certification. Any time you make software changes, you have to recertify the entire design, which can be costly in time and money. Code is also more difficult to test for implementation holes. One mantra of security validation is, "Doubling the number of lines of code doubles the effort required to keep the same level of assurance." One way to reduce the pain of upgrading a system is by tightening your security boundary. For example, you can place application code outside the security boundary. Once you show that a module is secure, regardless of the application code, you can change the application code without recertification. This strategy exemplifies what the security boundary is all about and why it is critical to carefully define it.

Once an attacker has physical access to a system, it is only a matter of time until he or she breaks it. Use time to your advantage and a variety of defenses to delay attackers. Remotely change your code

on a regular basis to keep your system a moving target. Limit the effect of system compromise. Don't base all your devices on a single key; otherwise, if someone breaks it in one device, it affects all of them. If you project that it will take six months to break a master key, then change keys every three months. Protect against well-known attacks before struggling with esoteric ones. Remember: No one is going to try to break through your fortress's front door if there's a window in the back.

Security requires a "good enough" approach. Your best defense is to raise the cost of an attack beyond the value of succeeding. You need to find the attacker's threshold of pain while exceeding your own as you design, manage, maintain, and update your system. Most of the time, a simple barrier is enough to keep honest people honest.

AT A GLANCE

* Given enough time, resources, and motivation, an attacker can break any system.

* Determine what you want to protect, from whom you want to protect it, and for how long you want to protect it.

* The best defense is to make the cost of breaking a system greater than the value of information an attack gains.

* Defining the proper security boundary is critical for designing a flexible yet provably secure system.

ACKNOWLEDGMENT

Thanks to Paul Kocher, president and chief scientist of Cryptography Research, and Christof Paar, from Ruhr-University Bochum and editor of Cryptographic Hardware and Embedded Systems 2002.

REFERENCES

(1.) Cryptographic Module Validation Program Conference 2002, March 2002, www.csrc.nist.gov/cryptval/cmvp2002/ index.html.

(2.) Derived Test Requirements for FIPS 140-2, csrc.nist.gov/cryptval/140-l/fips 1402DTR.pdf.

RELATED ARTICLE: Chip-level defense: memory.

Many encryption processors store keys off-chip, in these instances, volatile memory has a distinct advantage over nonvolatile memory. However, you can't count on simply cutting power to erase keys; you must overwrite keys, because a latent charge may hold a partial memory image. If you're storing a million security associations--which could mean 256 Mbytes of memory--can you zero the memory

quickly enough?

In secure applications, every bit must be reliable. For example, if an error occurs when a cryptographic engine stores a key in SDRAM, you lose the key for good. As technology processes get smaller, the risk that cosmic rays could flip bits increases. By writing an EEC (error-correcting code) in a separate memory every time you write data to memory, you can use the ECC when you read the data back to see whether any bits failed.

Liquid nitrogen is an effective way to quickly freeze and lock memory cells. To defend against a liquid-nitrogen attack, your device needs to detect low temperatures and react quickly to them.

RELATED ARTICLE: Chip-level defense: processors.
You can make breaking a board more difficult just by scratching off a chip's product number. But a more effective technique is to "pot" components and their leads. Potting makes a board "tamper-evident," meaning you can quickly tell whether someone has attempted to compromise it. Unfortunately, potting complicates upgrading and renders the board useless if any of the potted components fad. Attackers can mill off or remove epoxy coatings with chemicals.

Encryption chips often handle more cryptographic keys than a chip can efficiently store. Processors that encrypt keys before storing them off-chip pull the security boundary in tighter: The fewer copies of information and the fewer places information can reside, the more you limit its exposure. Most chips lack a mechanism to dump their contents; you need a processor to manage all sensitive data, tracking its location and actively destroying it in the case of tampering. These mechanisms expand your security boundary.

Reverse-engineering is legal. Companies should verify that you have a legitimate reason for reverse-engineering someone else's chip, such as to verify whether someone is violating one of your patents, but not all do. Don't count on secrets in your schematics remaining secret.

Once someone has your chip schematic, he or she can more easily probe internal buses on the die. You can make the process more difficult-but never impossible-by obscuring the layout of your chip. Spread out functional units. Also, fill in any spare room on the die with false traces, so that the attacker doesn't know which transistors matter. Unfortunately, though, doing so affects your simulation times and increases the possibility of problems when you move or add false traces. Another way to thwart probing is to keep cryptographic keys moving. Store them in revolving buffers or XORed against a pattern, so that their value at any given clock cycle is unknown.

In truth, complex chips with millions of transistors do fail over time.

It's hard enough to build a failure-resistant chip; it's even harder to prove that you've done so. Cryptography is intolerant of computational errors, and even a single transistor failure can expose unencrypted data. (XORing plain text against 0 yields plain text-not cipher text.) A failure can also destroy the data, because the system discards the original data after encryption, and the corrupted cipher text will not yield the original data. One method of detecting a data-destroying failure is to employ a redundant encryption engine; if you don't get the same results from both engines, a catastrophic failure has occurred. Running parity bits on every data line effectively provides a redundant bus. You can also periodically verify chip integrity by using BIST (built-in self-test) or sending test data through the chip.

One method for breaking processors is to subject them to extreme operating conditions in the hope that the processor will act in an unintended manner and reveal sensitive information. Extreme heat or cold, for example, can cause erratic behavior. Your defense is a temperature sensor.
Another attack involves cranking up the clock speed. A PLL, an overfrequency detector, or an underfrequency detector can sense this attack. The attacker may try introducing inputs that you never expected, such as invalid formats to crash parsers, non-real-world bursts to overflow buffers or stacks, or illegal commands over control buses to see whether the chip fails when you feed it garbage. The best protection against such attacks is to design a system than can accept every possible variation of input from interfaces across the security boundary. Also, make sure you haven't left any debugging code or traces in production code. Attackers can and will use JTAG or BIST ports against you.

Choosing a highly secure encryption chip has become more complex than comparing the speed of execution. For example, certain implementations use processor instructions that leak less information than instructions that traditional implementations use. Other methods of protecting processing include randomizing data during intermediate steps in an algorithm, employing nondeterministic execution of the sequence of instructions, or using decoy code to make it more difficult to understand what's happening inside the chip. You may want to force the chip vendor to provide details about how the algorithms are implemented to counteract certain known attacks.

A recently discovered class of attack, which attackers implement with an $8 laser pointer, is optical fault induction. During such an attack, an attacker can set or reset any individual bit of SRAM in a microcontroller (Reference A). The attacker can use the attack to set part of a key to a known value or to disrupt the integrity of cryptographic computations. One suggested defense uses self-timed dual-rail circuit-design techniques to encode a logical 1 or 0 as high/low or low/high on a pair of lines. The combination high/ high triggers an alarm indicating that an attack may be in progress. The

overall ramifications of optical fault inductions are still unknown.

Given the high probability that new attacks will occur after you implement a design, you should enable a secure method for updating both control and cryptographic processors. A literature search reveals that researchers have broken specific processors, and the appropriate vendors have responded with firmware revisions that correct such problems. However, if you cannot incorporate these corrections into deployed devices, those devices will be vulnerable to known and acknowledged attacks.

REFERENCE

(A.) Proceedings of the CHES (Cryptographic Hardware and Embedded Systems) workshop, August 2002, www.cheswork shop.org.

RELATED ARTICLE: Board-level defense.

Discovering the layout of a board requires only one spare board. An attacker can care. fully mill down potting and develop a schematic. Certainly, the attacker loses sensitive information when he or she mills down a board, but he or she can now use the schematic to compromise other boards. An X-ray machine may be able to more quickly provide the same information without sacrificing the board. For high-volume applications, such as set-top boxes, making several variations of your boards can limit the damage of a successful attack by reducing the number of similar boards that attackers can compromise. You can also create variations at the chip level; each time you spin a chip, you mix up the insides.

Boards radiate energy, enabling attackers to read the inductance of each pulse on each trace. Shielding can resist these attacks, as can running signal lines between ground planes, which, unfortunately, requires multiple-layer boards and increased cost. However, to achieve "tempest-shielding" levels, at which your board emits no radio easily exceed the value of the electronics it protects.

The "jigsaw" method scatters pieces of a key across a board or a chip so that attackers can't find it by looking in one location. Because this method of storing a key involves a secret algorithm, and all secrets can be broken, it makes finding keys more difficult but not impossible.

Meshes or grids that short-circuit when you penetrate them provide the most robust levels of protection. Thick welded metal also works well in applications in which elegance and low cost are not requirements. Consider adding a light sensor to check whether someone successfully penetrates the enclosure.

For low-end applications, such as point-of-sale machines, a tamper-

resistant switch may be sufficient. Because the machine contains sensitive data only when it is running, shutting down the machine effectively secures the sensitive data. However, attackers can easily find these switches with X-rays and drill them out.

An exposed bus isn't vulnerable only to sniffing. With enough motivation, an attacker can even force values onto the bus.

A secure subsystem involves many stages beyond design and validation. You need to integrate the secure subsystem into a nonsecure system; provide documentation and training defining proper use and installation of the subsystem, so as not to compromise its security through misuse; and develop a maintenance program that regularly confirms that the subsystem is still secure.

RELATED ARTICLE: Power attacks.

Zeroing memory after a power failure requires power, usually from a battery. The drain on batteries in secure modules--either to maintain keys when the power is off or to power key zeroing sequences when power is interrupted-is typically low, meaning that the projected batten/life is the projected shelf life of the battery. If the life of the board is longer than the shelf life of the battery, you need to work battery updating into the scheduled maintenance for the board. If the battery protects information such as keys, you must provide a mechanism to power the board to preserve the keys while you remove and replace the battery. With tamper-resistant enclosures, you need to select a battery with an extremely long shelf life or one that you can recharge without compromising the security of the board.

An attacker may try to break the leads to the battery before the system destroys sensitive data. (No joke: Bullets can effectively do this job.) Such an attack may occur while the board is powered, so you need to monitor the battery.
Determine whether your board will have to tolerate a power-down situation, such as for service on nonsecure parts of the board. If so, you cannot use a power failure to trigger a response.

Currently, you can't put batteries on a chip. If you need to be able to zero memory on a chip or have that chip zero on-chip memory, you need an external battery. Thus, your security boundary will mostly likely never be a single chip.

Expand your thinking about what it means to cross the security boundary. For example, power-analysis attacks use statistical techniques to gather information on variations in power consumption and signals. For example, the power consumption on a trace may go up if the first key bit is 1. Some defenses are to increase the SNR and to use complementary logic to mask the power signature. Automated testing overcomes the noise defense, because an attacker can increase the number of samples he or she takes. You

should assume that a certain amount of information leaks whenever you perform an action. One defense is to change keys once per transaction; the attacker gets a little information during each transaction but has no way to combine it. Note that power analysis is an effective attack on simple systems, such as smart cards, but it becomes less of a threat as chip complexity rises.

HUMAN FACTORS

People are reliably unreliable. However, if they never know a cryptographic key, they can't "accidentally" tell it to someone else. You don't find a lot of off-the-shelf software to manage keys at the chip level-a serious hole in the product line for most cryptographic<hip vendors-yet key management plays a critical role in preventing people from compromising the key security. Don't underestimate the challenge of software-key management or its role in FIPS-140-compliance testing.

Any tamper response you deploy should account for the fact that people make mistakes. For example, a technician might accidentally remove a secure board and then try to quickly replace it. if the board has zeroed its memory, the technician has to go through the long process of reconfiguring the board.

Some of the most effective attacks have nothing to do with cryptography but instead focus on flaws in the protocols that manage keys. For example, the master keys for a board are often generated and stored during the manufacturing process. An unscrupulous line worker might be persuaded to compromise the integrity of the line. Thus, you need a key-management system that ensures that no human has ever had knowledge of the key.

Some keys are worth little However, a master key that controls many other keys is worth stealing. Certainly, master keys facilitate key management, but they upset the balance of the effort to steal it versus the payoff. One method of protecting master keys is a consensus escrow, in which several people or tokens have only a piece of the master key. To use the key, a quorum of the group must meet. For the key to be lost, several people must compromise it.

Attackers sometimes are on the inside--people who have intimate knowledge of and legitimate access to secure systems, the best defense against such attackers is to assume that they exist and will attack the system. And be aware that stealing a password by looking over another person's shoulder has reached new heights. Obtaining system passwords is easy. Try the Key Katcher, a small dongle attached between the keyboard and the computer that can store 64,000 keystrokes and is available at www.thinkgeek.com You might consider creating an awareness program for your customers, showing which of their actions may compromise the security of the system.

TAMPER-RESPONDENT SENSORS

Tamper-respondent sensors, such as WL Gore's D sensors and enclosures, defend the physical security boundary of a module, the sensor comes as a wrappable, foldable sheet that stretches around edges and corners of a module without making these areas more vulnerable to attack. An organic and conductive ink crisscrosses through the sheet with a maximum distance between traces of 200 to 300 microns, and the electrical state of the sensor changes if the field is broken, triggering tamper-respondent mechanisms, such as zeroing key memory (Figure A). The ink is invisible to X-rays, which you can use to find openings in wire meshes. An opaque resin coating prevents attackers from seeing the traces. Any chemical able to destroy the resin can also destroy the ink.

[FIGURE A OMITTED]

The sensor needs a battery consuming only microamps to stay active when the board is not powered. Window comparators around the sensor trigger when the field changes. You can use a microcontroller unit to scan the comparators to prevent a transient event from triggering a defensive response. This step is especially important if your board contains a small explosive, which it can use to destroy itself.

One drawback of using tamper-respondent sensors is that they make it impossible to troubleshoot modules. Another drawback is that the resin coating is a poor thermal conductor, so design of the overall package becomes important. Hot devices must directly contact the metallic inner casing and thus spread heat across the greatest possible area. You might paint the encapsulated module black to radiate heat, attach an external heat sink, or place the module in an airflow. Note that a heat attack can compromise external cooling methods, suggesting the use of a heat sensor. However, be careful to set your temperature thresholds so that the module doesn't interpret a failed fan as a physical attack.

WL Gore must shape the D' tamper-respondent sensor for each application so it fits efficiently. Prices start at approximately $50 (thousands per month) for a small device.

PROTECTING IP

Cryptographic keys and credit-card numbers aren't the only information worth protecting. For many design companies, the value of the company lies in its IP (intellectual property). Some attackers seek to learn about the actual system. From a hardware perspective, many defense methods can effectively protect board layout. Software and FPC, A cores, however, are significantly more vulnerable to theft.
Two aspects of software vulnerability are the degree to which the software is exposed and the software's portability. For example, an

attacker can lift code or cores stored in EPROM or flash memory using a scope when a CPU or an FPGA accesses them. More secure is a processor with write-only, nonvolatile memory that can't download the code stored inside. The portability of code or cores refers to the usefulness of the raw IP. An attacker can alter code to create a rogue upgrade that exposes otherwise-secure information. Then again, a user may be interested only in the ability to use the captured data as is. For example, the attacker may want to simply copy a core into an FPGA to use as a black box without paying licensing fees.

Xilinx, for example, addresses the vulnerability of FPGAs through an on-chip 3DES decryption engine in its Virtex II and later product lines. You en crypt the core before storing it in nonvolatile memory. Because the FPGA must have the correct keys to decrypt the core, an attacker cannot simply copy the core into another FPGA; he or she must extract the keys from the FPGA before copying makes sense. Note that, when you use encryption, the FPGA disables read-back and partial-reconfiguration features, which would help attackers work out the schematic of the core.

One vulnerability of the Xilinx scheme is the volatility of the 3DES keys. Placing nonvolatile memory on the FPGA would affect overall device performance. Preserving keys when there is no power requires a battery. If you remove this battery, the FPGA resets the keys. An attacker can then load in new keys and a new configuration. (Note: Creating a new configuration isn't trivial and may require access to design notes and documentation.) Unless the system has a mechanism elsewhere to watch the FPGA change configuration, such tampering may not be evident. Any upgrades sent to the FPGA will fail because the keys are wrong, and the spoofed core will likely acknowledge a successful upgrade to prolong the deception. Furthermore, you lose access to the FPGA and may be able to defeat the rogue upgrade only by physically resetting the device.

FOR MORE INFORMATION

For more information on products such as those discussed in this article, go to www.edn.com/info and enter the reader service number. When you contact any of the following manufacturers directly, please let them know you read about their products in EDN

Broadcom
1-949-150-8700
www.broadcom.com
Enter No. 317

Corrent
1-480-648-2300

www.corrent.com
Enter No. 318

Cryptography
Research
1-415-397-0123
www.cryptography.com
Enter No. 319

Hifn
1408-399-3500
wwwv.hifn.com
Enter No. $20

nCipher
1-181-994-4000
www.ncipher.com
Ehter No. 32i

Precidia
Technologies
1-613-592-7557
www.precidia.com
Enter No. 322

Rainbow
Technologies
1-949-450-7300
www.rainbow.com
Enter No. 323

WLGore
1-888-914-4675
www.wlgore.com
Enter No. 324

Xilinx
1408-559-7778
www.xilinx.com
Enter No. 325

OTHER RESOURCES

CESG (Communications
Electronics
Security Group)
www.cesg.gov.uk

Common Criteria
www.commoncriteria.org

Cryptographic Module
Validation Program
www.nist.gov/cmvp

CSE (Communications
Security Establishment)
www/cse-cst.gc.ca

FIPS 140-2
specification
http://csrc.nist.gov/
publications/tips/
fips140-2/fips1402.pdf

NIST (National Institute
of Standards and
Technology)
www.nist.gov

SUPER INFO NUMBER For more information on the products available from all of the vendors listed in this box, enter no. 326 at www.edn.com/info

---

Business Wire May 3, 1999

Box Hill Teams With Mercury to Expand SAN Software Offerings.

NEW YORK--(BUSINESS WIRE)--May 3, 1999--

Box Hill Systems Corp. (NYSE: BXH), a leading independent provider of storage and SAN solutions, has teamed up with Mercury Computer Systems, Inc. (NASDAQ: MRCY) of Chelmsford, MA to provide SANergy(TM) software, which allows files to be shared on Storage Area Network (SAN)-based storage, using standard networks and file systems. SANergy transcends platforms and file systems simply and transparently at full SAN speeds.

"Our customers demand comprehensive, state-of-the-art SAN software solutions," said Philip Black, Box Hill's CEO. "By integrating SANergy into our offerings we provide our customers with fully integrated hardware and software SAN Solutions."

Specifically designed to extend industry-standard file systems, protocols, and Storage Area Networks, Mercury's SANergy delivers the full file-sharing capabilities of LAN-based file servers at the high-speed data throughput of a SAN. The software maintains network-based access controls and data integrity across multiple operating systems without the bottleneck imposed by a file server. This allows SANergy to accelerate most I/O-intensive applications, including streaming multimedia, prepress "direct-to" workflows, data mining, and multi-server Web hosting. SANergy supports UNIX, Windows NT and Mac OS platforms.

"As one of the worldwide leaders in storage and SAN solutions, Box Hill brings our company an unparalleled level of expertise in integrating software and hardware SAN products," said Barry Burke, vice president and general manager of Mercury's Shared Storage Business Unit. "This expertise is invaluable to those customers requiring an integrated SAN solution."

Box Hill Systems Corp. is a leading independent provider of storage and SAN solutions. Box Hill, based in New York City, is recognized by

a customer base that includes many of the largest financial telecommunications, digital imaging, multimedia, pharmaceutical, government and university research institutions in the world. Box Hill's home page is www.boxhill.com.

Box Hill and the Box Hill logo are trademarks or registered trademarks of Box Hill Systems Corp. SANergy is a trademark of Mercury Computer Systems, Inc. All other products mentioned herein are trademarks or registered trademarks of their respective owners. -0- Certain statements contained in this press release, including statements regarding the business, the intent, belief or current expectations of the Company, its directors or its officers, primarily with respect to the future operating performance of the Company and the products it expects to offer and other statements contained herein regarding matters that are not historical facts, are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act. Because such statements include risks and uncertainties, actual results may differ materially from those expressed or implied by such forward-looking statements. Those risks and uncertainties include, among others: rapid technological change, frequent new product introductions, evolving industry standards and changing customer preferences in the Open Systems storage market. In addition, the Company's business and results of operations are subject to numerous additional risks and uncertainties, including: availability and cost of key components; dependence on a limited number of customers; reliance on the financial services and telecommunications industries; ability to attract, train, retain and motivate qualified management, technical, manufacturing, sales and support personnel, demand on administrative, operational, financial, manufacturing, sales and customer service resources caused by the Company's growth and expansion; and, the Company's ability to protect its proprietary software and other intellectual property rights. Additional risks and uncertainties that Box Hill Systems faces can be found in the form 10K most recently filed by the Company. All forward-looking statements speak only as of the date on which they are made. Box Hill undertakes no obligation to update such statements to reflect events that occur or circumstances that exist after the date on which they are made.

PR Newswire April 10, 2003

Microsoft announces first Windows CE Shared Source Program to allow commercial distribution of modified source code.

Author/s:

Redmond, Washington -- Redmond, Washington, April 10 /PRNewswire/ -- - Program Garners Widespread Support From Industry Leaders Such as ARM, Hitachi, Intel, Mitsubishi Electric and Samsung, Citing New Business Opportunity and Customer Benefit

Microsoft Corp. today announced the latest addition to its Shared Source Initiative, the Windows(R) CE Shared Source Premium Licensing Program (CEP), available to companies that are bringing Windows CE-based devices and solutions to market. CEP is the first Windows CE program under the Shared Source Initiative to allow original equipment manufacturers (OEMs), silicon vendors and systems integrators full access to Windows CE source code. All licensees will be able to modify the code, and OEMs now can commercially distribute those modifications in Windows CE-based devices.

Many industry-leading companies such as ARM Ltd., BSQUARE Corp., Hitachi Ltd., Mitsubishi Electric Corp., MIPS Technologies Inc. and Samsung Electronics have already joined the program and are developing innovative and differentiated embedded products. Companies such as Hitachi already have begun shipping devices based on Windows CE with modifications under the CEP.

"Premium source code access is vital to enabling our long-standing optimisation efforts around Windows CE .NET on the ARM architecture," said Mike Muller, chief technology officer at ARM. "The results enabled by this program directly translate into competitive advantage delivered to the entire ARM partnership. Premium source access, along with our on-site people in Redmond, has increased the effectiveness of our collaborative efforts. We have had an excellent experience and fully support Microsoft's efforts in this area."

"The Microsoft(R) Windows CE Shared Source Premium Licensing Program enabled Hitachi to work directly with the Windows CE .NET source code and modify certain aspects of the operating system to create a truly enhanced user experience, specifically for one of our new mobile devices," said Shigeru Matsuoka, general manager of the Mobile Information & Communication Appliance Division, Ubiquitous Platform Systems, Hitachi Ltd. "Having the rights to modify the Windows CE .NET source code allows us to bring optimised and differentiated devices to market quickly."

"The Shared Source Initiative is about learning from our customers and the community to provide enhanced source-code transparency plus the ability to do more with your Microsoft-based solution," said Craig Mundie, senior vice president and chief technical officer of Advanced Strategies and Policy at Microsoft Corp. "We continue to see tremendous growth and interest in Windows CE Shared Source offerings, and the new CEP is designed to meet the needs of our customers and their desire to innovate and expand on the Windows CE platform to deliver new business and industry opportunities."

- CEP Designed for Innovation, Empowerment and Community

Full access to the source code and rights to modify and ship the code commercially enable licensees to build on top of the rich Windows CE foundation to create new and innovative devices. Shared Source Premium code empowers licensees to optimise and differentiate software and hardware for Windows CE. CEP also includes a customer feedback program, which enables customer collaboration and community contribution to ongoing improvements to Windows CE products. More information about CEP can be found at http://www.microsoft.com/resources/sharedsource/licensing/windowsce_announcement.mspx.

- Windows CE Shared Source Licensing Program

CEP builds on the successful Windows CE Shared Source Licensing Program, from which more than 160,000 lines of Windows CE Shared Source code have been downloaded. The program allows developers, researchers, students and other interested parties to use the Windows CE Shared Source code for any non-commercial purpose, including creating and distributing derivatives. In addition, for commercial purposes, the source code enables customers to develop, debug and support their own commercial software and hardware for the Windows CE platform. More information on this program and the new Windows CE Shared Source Premium Licensing Program can be found at http://www.microsoft.com/licensing/sharedsource/.

- About the Shared Source Initiative

The Microsoft Shared Source Initiative is a balanced approach that makes source code more broadly available while preserving the intellectual property rights that sustain a strong software business. The Shared Source Initiative framework supports a spectrum of programs and licenses offered by Microsoft to customers, partners, developers, academicians and other interested individuals.

Each source-licensing program under the Shared Source Initiative is tailored to the needs of a particular Microsoft constituent community and can be applied as a model for increasing code transparency throughout commercial software. Shared Source is an evolving framework that will support additional source-code access programs and licenses involving many Microsoft product groups. Currently, Windows 2000, Windows XP, Windows Server(TM) 2003, Windows CE 3.0, Windows CE .NET, Microsoft Passport Manager, and components of Visual Studio(R) .NET and ASP.NET have source code available through the Shared Source Initiative.

- About the Microsoft Embedded and Appliance Platforms Group

Microsoft Windows Embedded operating systems and tools provide comprehensive software platforms for building the next generation of intelligent, 32-bit connected Windows Powered devices that demand rich applications and Internet services for a wide range of flexible solutions. In addition, Microsoft offers a wide range of programs and services designed to meet the specific needs of Windows Embedded customers, industry partners and developers. The Windows Embedded operating systems currently include Windows CE and Windows XP Embedded. The Server Appliance Kit for Windows 2000 helps OEMs build Windows Powered server appliances, including network attached storage (NAS) and Web servers. Windows CE was honoured at the 2003 International Consumer Electronics Show for innovations in the category of Software/Embedded Technologies. The Embedded and Appliance Platforms Group also delivers Windows CE for Smart Displays software technology, which powers a wide range of Smart Displays that extend the Windows XP experience to any room in the home. Currently in development is "Media2Go," which is the code name for a new device platform for powering the next generation of portable media player devices that enable consumers to enjoy their videos, music and pictures on the go.

- About Microsoft

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software -- any time, any place and on any device.

Windows CE Shared Source Premium Industry Quotes

"Microsoft's Windows CE Premium Source offering allows our software engineers to closely examine the interaction between their code and the operating system, and to generate various derivatives of the operating

system components for testing purposes. These capabilities help them develop better drivers and applications, and better support our customers' Windows CE-based product development and troubleshooting efforts."

-- Tom Gensel
Chief Software Architect
Accelent Systems Inc.

"Premium source gives our developers the ability to understand the interactions between the Windows CE operating system and the custom code that we develop. Using premium source, we can develop code much faster and at a higher level of quality, which allows us to get our products to market much faster."

-- Brian Crowley
Vice President of Product Development
BSQUARE

"As a gold level Windows Embedded systems integrator, we have used the Windows CE Shared Source Premium source code to better understand the Windows CE Kernel and device drivers. With this source code knowledge, we were able to develop more stable and reliable device drivers including those for the CDMA EVDO Wireless Modem and CDC (Communication Device Class) wireless modem."

-- Bejay Ahn
CTO

DST Corp.

"Participation in the Microsoft Windows CE Shared Source Premium Licensing Program has provided Intel with a unique opportunity to enhance Windows CE .NET-based solutions based on the Intel XScale technology. The program will help provide significant improvements to leading-edge solutions that showcase our respective technologies."

-- Hans Geyer
Vice President and General Manager
PCA Components Group
Intel Corp.

"Intrinsyc's participation in the Windows CE Shared Source Premium Licensing Program provides important company and customer benefits. Because our development team has access to Windows CE .NET premium source code, it can test ideas and speed the debugging and systems integration processes. This results in intelligent devices that are ready for market faster and optimised for performance."

-- Neil McDonnell
President and CEO
Intrinsyc Software Inc., a Microsoft Gold Level Embedded Partner

"The announcement of Windows CE Shared Source Premium Licensing Program provides new opportunities for MEI to

use Windows CE .NET in fields such as digital consumer electronics products, where rapid growth is expected. We believe that the advanced network and multimedia functionalities of Windows CE will bring more enhanced value-add to our semiconductor products."

-- Masashi Deguchi
Director,
Software Development Center
Corporate
Development Division
Semiconductor
Company
Matsushita
Electric Industrial Co., Ltd

"An important part of the MIPS Alliance for Windows CE is the opportunity for MIPS Technologies and many of the world's leading semiconductor companies to work closely with Microsoft to optimize Windows CE .NET for the industry standard MIPS architecture. By expanding the availability of Windows CE .NET through the Shared Source Premium program, Microsoft will broaden the base of designers using its technology as the RTOS of choice in next-generation digital consumer and networking applications."

-- Brad Holtzinger
Director of
System Solutions
MIPS Technologies

"As technology for mobile and high-performance network devices advances,

Mitsubishi Electric combines its technology and expertise with Microsoft's Windows CE .NET embedded operating system to more rapidly bring products to market. Mitsubishi Electric views the Windows CE .NET Shared Source Premium Licensing Program as an outstanding offering that can advantageously profit the companies that use it."

-- Satoshi Tanaka
Manager, Internet Media Systems Dept.
Information Technology R&D Center
Mitsubishi Electric Corp.

"The Premium Source Licensing program, coupled with an emphasis on collaborative development within the Windows Embedded Group, has provided significant benefit to both National Semiconductor's Information Appliance Division and Microsoft. The level of expertise for our engineers in developing optimised silicon and software for Windows CE has increased dramatically. Our visibility into the source has enabled us to effectively collaborate with Microsoft to greatly improve performance and stability on our platforms."

-- Jeff Lavin
Director of Engineering
National Semiconductor Corp.

"With technological innovation

accelerating the advancement of mobile devices and high-performance network devices in the marketplace, timely product development is very important in order to keep up with market needs. Realizing that software and the operating system play a key role, NEC AccessTechnica highly appreciates Microsoft Windows CE .NET and subsequently has adopted it for its advanced features and functionality. NEC AccessTechnica also highly appreciates the superior advantages of Microsoft's Windows CE Shared Source Premium Licensing Program. Combined with NEC AccessTechnica's technology and expertise, it enables us to rapidly bring a product with enhanced value to the market. It has the merit of being open source, while protecting the software's intellectual property. It is seen as an outstanding offering that provides advantages to the companies that use it. NEC AccessTechnica plans to continually extend this offering to future product development on an ongoing basis."

-- Katsuaki Ohwada
General Manager
Solutions Product Development Division
NEC AccessTechnica Ltd.

"Providing optimised and timely solutions at low cost while responding to user needs and using the latest technologies is a significant differentiating factor in the industrial device industry. At NEC

Infrontia, Windows CE .NET's cutting-edge technology develops i-Communication Systems, i-Appliances, and i-Solutions systems.

Microsoft's recently announced Windows CE .NET Shared Source Premium Licensing Program has enabled NEC Infrontia to take an industry lead and quickly bring to market business terminals, such as the Pocket@i with built-in wireless LAN, PHS, and laser scanner. NEC Infrontia is eager to continue aggressively using Windows CE .NET and its shared source program in our company's core enterprise areas."

-- Eiichi Kumagai
Associate Senior Vice President and General Manager
Second Operations Unit
NEC Infrontia Corp.

"With access to the Windows CE Shared Source Premium code, Samsung is able to easily incorporate customer requests into devices, create even more innovative products, and decrease the development cycle and time to market for Digital Home devices."

-- Young Koo
Director, Digital Media R&D Team
Samsung Electronics

"The Windows CE Shared Source Premium Licensing Program allows us to quickly react to our customers'

requests for development. The program enhances our ability to develop innovative wireless and wired projects utilizing Microsoft Windows CE technologies."

-- Kevin Wixom
Vice President of Embedded Product Development Group
Stellcom Inc.

"3SOFT views the Microsoft Windows CE Shared Source Premium Licensing Program as a positive initiative. With access to Windows CE .NET source code, we now are able to quickly support our customers with operating system questions or debugging issues on the highest-possible technical level."

-- Martin Schleicher
Head of the Man Machine Interfaces Division
3SOFT GmbH

"The Premium Source Program enables Toshiba to work with Microsoft and MIPS Technologies to optimize and enhance the Windows CE .NET kernel and tool chain. These activities will provide more powerful and flexible MIPS-based solutions for OEMs and customers in emerging digital consumer markets."

-- Masayasu Odani
Chief Specialist, System Platform Development Department, System & Software Division Semiconductor Company
Toshiba Corp.

"As a gold-level system integrator for Windows Powered solutions, having access to the Windows CE source code allows us to help customers to market faster and for less cost. The Windows CE Shared Source Program allows developers to open the proverbial 'black box.' The ability to watch how the system code is interacting with and manipulating user code and data is an extremely powerful and time-saving tool during test and development."

-- Daron Underwood
Principal Engineer and Consultant
VenturCom Inc., and Microsoft eMVP

"We are delighted to be participating in the Microsoft Windows CE Shared Source Premium Licensing Program. By giving us timely and convenient access to the source code, it enables us to optimize our embedded platforms and speed up our time to market."

-- Richard Brown
Associate Vice President of Marketing
VIA Technologies Inc.

"As a gold-level Windows Embedded Partner (WEP) and Shared Source Premium partner, Vibren now will be able to develop and distribute innovative, customisable enhancements of Windows CE source code to our customers.

This increases our value-add and helps us expand our business."

-- Dave LeClair
Vice President of Technology

Vibren Technologies Inc.

Note to Editors: If you are interested in viewing additional information on Microsoft, please visit the Microsoft Web page at http://www.microsoft.com/presspass/ on Microsoft's corporate information pages. Web links, telephone numbers and titles were correct at time of publication, but may since have changed. For additional assistance, journalists and analysts may contact Microsoft's Rapid Response Team or other appropriate contacts listed at http://www.microsoft.com/presspass/contactpr.asp.

Deborah Sommer, 425-638-7000, deborahs@wagged.com, Mark Martin, 503-443-7000, markm@wagged.com, or Rapid Response Team, 503-443-7070, rrt@wagged.com, all of Waggener Edstrom

---

Dec, 2000

The key to future success.

Author/s: Steve Everhard

The things that make the Internet so attractive - openness and anonymity - pose a threat to its future success, warn Steve Everhard and Keith Saunders

It seems that e-commerce is everywhere these days. You name it - everything can, and is being accomplished electronically. Yet the very features of openness, anonymity and global reach that make the Internet so attractive are major barriers to the adoption of electronic commerce for many companies and consumers because of the huge opportunities for fraud and deception.

To complete a transaction over the Internet, we need to be able to trust that the company we are negotiating with is both who it says it is and an organisation with whom we can safely and legitimately do business. Of course, this is a two-way street and any merchant needs similar assurances about a prospective buyer. At the same time we need to establish a channel for communications that protects us from eavesdroppers who may be able to exploit the trading relationship fraudulently.

The world of cryptography offers the Internet-enabled business a palette of tools to protect communication and commerce, but to determine their effectiveness we need to understand a little of what they do and, like any form of defence, what their vulnerabilities are.

Cryptography is the science of modifying information to render it unreadable by casual observers yet allowing the recipient to recover the message simply and reliably. The mathematical function used to encrypt and decrypt information is called a cryptographic algorithm, or cipher. Practically all modern cryptographic schemes make use of a

unique numeric sequence called a "key", which allows the specifics of the algorithm to be available freely as the security lies in protecting the key and not the way its applied.

The most common type of "symmetric" encryption in use today is called DES (data encryption standard), which is used widely in banks and business as well as networks. DES uses a relatively simple scheme that can be easily implemented in general purpose computers and yields fast results but, unfortunately, takes only minutes for a professional hacker to crack.

About 10 years ago a symmetric algorithm called IDEA (international data encryption algorithm) was developed using a similar scheme to DES. It is about twice as fast to encrypt information and more difficult to crack as there are twice as many key combinations to try, so it would take longer than the age of the universe to complete using current techniques. Although this sounds like good news, undoubtedly more sophisticated attack techniques will appear as the algorithm becomes more popular. The inherent weakness of all symmetric schemes remains the use of a single key for encryption and decryption.

The "asymmetric" algorithms, also known as public key (PK), use two keys in their cryptographic system, and the best known implementation is RSA. Unlike the symmetric systems where security relies on having to try every possible key combination, the asymmetric system depends on it being computationally not feasible to identify the private key from the public. The bad news about using long keys is that it takes longer and longer to encrypt and decrypt.

Digital signatures are used to determine the origin of a document. They normally work by using a one-way hashing algorithm in such a way that it is almost impossible for two messages to hash to the same value, giving us a document "fingerprint" much smaller than the original document. The hash is then encrypted with RSA. The hash value can be proof of ownership of the message without the document itself being available, or it can be used to prove no changes to a reviewed document have been made. The result is that both the integrity of the document and its ownership are assured.

The technology used to sign the document must be useable in any end-point device (PC, phone, card terminal) and there should only be one copy of the private key as multiple copies cause unnecessary technology and infrastructure complications as well extra security loopholes.

How can the signature technology be proved to be secure? To assure the private key's integrity it is critically important that the key never leaves the token once it has been stored there. Ideally, rather than act as a storage device, the token should generate the public/private

keys itself and then manage distribution to those who need to validate the signatory's identity. Placing key management responsibility on the token removes another potential security loophole and makes it easy to issue multiple key pairs for different applications.

The only portable and interoperable security token that fits these needs and can be deployed universally in end-point devices is the smart card. The smart card provides a standardised set of physical and logical interfaces (defined by the ISO 7816 specification) and, being the same size, shape and weight as a credit card is highly portable.

The smart card holding the private key provides one of the three basic security requirements (something you have). There also needs to be a mechanism for proving the signatory has access to the private key using some sort of secret (something you know) - such as a PIN number - or a biometric (something you are). These mechanisms must be verified on the smart card to give a secure solution.

Modern multi-application smart cards - such as Javacard and Multos - allow the storage of multiple applications on one card, with the applications separated from each other by firewalls, making life simpler for the end user. As long as the end-point device knows which identity to pick, the user does not need to the detail. The key to this ability is the security mechanisms used to create the firewalls and the level of security awarded to the platform in independent testing. Change is inevitable, so the ability securely to add or remove identities to a card already issued is highly valuable. The newer smart cards support the dynamic loading and deletion of applications over insecure networks, allowing smart cards to be kept up to date with the user's lifestyle, rather than inhibiting changes as many other technologies do.

No other technology is secure enough to pass the tests required in a law court to support non-repudiation. None of the other security tokens -- plug-in cards or USB tokens -- have the breadth of acceptance in endpoint devices, or the security and application level flexibility required by a changing e-commerce landscape.
Of course the smart card holding the private key is only one part of any system designed to provide non-repudiation. We now have to surround the encryption with a system that defines the way in which keys are issued, recognised and managed. The most common RSA-based scheme is called public key infrastructure (PKI) and provides a standard mechanism through which all parties can obtain their cryptographic keys, as well as assuring confidentiality and integrity in how they are stored. This is done by establishing a trusted intermediary that can independently validate the signatory's identity and then signs the public with their own digital signature. A public key certificate is issued by a certification authority (CA) which includes the CA's own public key so the user can validate other

certificates issued by the same CA.

Alternatively a database (certificate repository) of known, authentic public keys and identities can be stored and used to validate signatures. The systems to archive transactions and contracts must also be capable of storing and retrieving all the information used to validate the signature.

Next, the systems used to unlock the smart card and generate the transactions and contracts must be designed so the correct information is presented to the card to sign. It is essential to ensure that the complex software used to deliver the information for signature to the smart card is secure, or all the effort put into securing the private key is wasted.

Establishing trust between trading bodies is complex and time consuming. Identrus LLC has built on the PKI scheme to establish a single trusted authority that certifies compliant financial institutions (FI) to a common and "technology agnostic" specification, as well as formal business processes. FIs issue digital certificates to their corporate customers that act like passports for trusted e-commerce transactions.

In the Identrus model, the Identrus CA is the cornerstone of the trust model. It issues CA certificates to its level 1 member financial institutions. This allows them securely to identify themselves to one another as being Identrus enabled. The CA also manages the registration of certificates by the RA (registration authority), ensuring that their status (active/revoked) is kept up to date. The status of certificates and communication of their status is managed by CRLs (certificate revocation list) and OCSP (online certificate status protocol) servers.

New trading partners subscribing to Identrus get a real-time assurance of the financial health of each other through their sponsoring FIs and can transact business whose value is guaranteed by an Identrus certificate. The shell of commercial certainty and assurance does much to support non-repudiation.

The Identrus corporate customer has its own Identrus guaranteed identity. This is presented in the form of a pair of certificates, and two sets of RSA key pairs stored on a smart card. Each corporate customer is given an identity certificate and a utility certificate. The identity certificate enables the customer to prove who they are; the utility certificate is used when executing "support applications", such as SSL (secure socket layer) authentication, or S/MIME data types. These certificates are accessed by client software and a reader, which together form what Identrus has termed "the black box".

Technological innovation has begun to provide a more trusted environment for e-commerce. For organisations considering issuance

of smart card technology the choices of technology are becoming clearer.

The environment is changing rapidly, which means today's applications may not meet tomorrow's business needs quite as well. The ability to add and remove applications to issued cards securely, and the capability for the card to adapt to its infrastructure by managing key pair generation will be major competitive advantages going forward.

Steve Everhard is commercial and marketing director and Keith Saunders is vice-president of business development at America's Maosco Consortium

---
